R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

PCT/FR99/02690

4

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

09/856191

REC'D 29 NOV 1999
WIPO PCT

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA RÈGLE 17.1.a) OU b)

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 16 NOV. 1999

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 17 NOV 1998

N° D'ENREGISTREMENT NATIONAL 98 14409

DÉPARTEMENT DE DÉPÔT 75

DATE DE DÉPÔT 17 NOV. 1998

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

SCHLUMBERGER SYSTEMES
Test & Transactions
50 Av. Jean Jaurès - B.P 620-04
92542 MONTROUGE Cédex
A l'attention de Anne DANG TRAN

n°du pouvoir permanent PG07391 | références du correspondant 76-0538 | téléphone 01 47 46 72 14

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale : ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☒ non

Titre de l'invention (200 caractères maximum)

DISPOSITIF POUR LA LIMITATION DE FRAUDES DANS UNE CARTE A CIRCUIT INTEGRE

3 DEMANDEUR (S) n° SIREN 5 6 2 1 1 3 5 3 0 code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

SCHLUMBERGER SYSTEMES

Forme juridique

Société Anonyme

Nationalité (s) Française

Adresse (s) complète (s)

50, avenue Jean Jaurès
92120 MONTROUGE

Pays

France

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande
SANS			

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire - n° d'inscription)

Anne DANG TRAN
Mandataire
(PG07391)

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

76-0538

N° D'ENREGISTREMENT NATIONAL

98 14 409

TITRE DE L'INVENTION :

DISPOSITIF POUR LA LIMITATION DE FRAUDES DANS UNE CARTE A CIRCUIT INTEGRE

LE(S) SOUSSIGNÉ(S)

Anne DANG TRAN
SCHLUMBERGER SYSTEMES
Test & Transactions
50, avenue Jean Jaurès - BP 620-04
92542 MONTROUGE Cédex

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

GUION Christian
5, le Clos
91370 Verrières le Buisson

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Le 22 décembre 1998

Anne DANG TRAN
(PG 07391)

BA 113/140897

DISPOSITIF POUR LA LIMITATION DE FRAUDES DANS UNE CARTE A CIRCUIT INTEGRE

La présente invention concerne un dispositif à circuit intégré contenant une zone mémoire comprenant une mémoire de données.

Un tel dispositif à circuit intégré est le plus souvent utilisé pour des applications dans lesquelles la sécurité du traitement d'informations est essentielle. Il s'agit en particulier de cartes à circuit intégré comportant des applications concernant le domaine de la santé, de la téléphonie mobile, ou encore, des applications relatives au domaine bancaire.

Une carte à circuit intégré se compose d'un corps de carte plastique dans lequel est incorporé un module électronique. Ladite carte communique avec un terminal, par exemple, un téléphone mobile, un terminal bancaire ou encore un ordinateur, via un réseau de communication et peut envoyer des messages contenant une information chiffrée audit terminal via ce réseau afin de sécuriser un transfert d'informations. Dans le langage courant, on dit que le message est signé. Pour le calcul de l'information chiffrée, la carte utilise une clef secrète de codage qui se trouve dans la mémoire de données de sa zone mémoire et un algorithme de cryptage.

Bien que le transfert d'informations soit ainsi sécurisé, une carte à circuit intégré reste vulnérable dans la mesure où un fraudeur peut effectuer un grand nombre d'actions sur la carte qui vont lui permettre de percer ses secrets. Ainsi, ledit fraudeur, désirant trouver ladite clef de codage, peut par exemple envoyer une instruction de signature d'un message à ladite carte et conserver la trace des signaux engendrés lors de l'exécution de ladite instruction. Par la suite, il peut envoyer un grand nombre d'instructions de signature du même message, soumettre la carte à des perturbations électromagnétiques à des instants précis du déroulement dudit algorithme et conserver les traces des différents signaux émis. En établissant une correspondance entre les traces de

signaux obtenues lors de perturbations et la première trace, ledit fraudeur peut étudier les différences ou l'absence de différences entre les diverses informations chiffrées obtenues pour découvrir une partie de la clef de codage. Ainsi, malgré le transfert d'informations sécurisées assuré par la carte, ledit fraudeur peut tout de même accéder à des informations confidentielles en effectuant un nombre très important d'actions sur la carte à circuit intégré.

Aussi, un problème technique à résoudre par l'objet de la présente invention est de proposer un dispositif à circuit intégré contenant une zone mémoire comprenant une mémoire de données, dispositif qui permettrait de mieux sécuriser la carte en limitant le nombre d'actions possibles sur la carte de la part d'un fraudeur.

Une solution au problème technique posé consiste, selon la présente invention, en ce que ladite mémoire de données contient au moins un élément compteur, au moins un élément indicateur et au moins une valeur seuil, ledit élément compteur comptant, d'une part, au moins un nombre d'occurrences d'événements survenus dans ledit dispositif, et, étant, d'autre part, susceptible d'atteindre ladite valeur seuil indicatrice d'un nombre maximum élevé d'occurrences desdits événements, ledit élément indicateur étant apte à passer d'un premier état à un second état lorsque ledit élément compteur a atteint ladite valeur seuil.

Ainsi, comme on le verra en détail plus loin, le dispositif de l'invention permet de limiter un nombre d'actions ou d'événements possibles sur ladite carte à circuit intégré grâce, d'une part, à un élément compteur qui comptera le nombre d'actions effectuées en prenant en compte une action ou un groupe d'actions, et, d'autre part, grâce à un élément indicateur qui indiquera qu'une valeur seuil d'occurrences d'événements ou d'actions a été atteinte ce qui permettra par la suite de sanctionner un prochain dépassement de ladite valeur seuil.

La description qui va suivre au regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est un schéma d'un dispositif à circuit intégré selon l'invention, ici une carte à circuit intégré.

La figure 2 est un schéma représentant une zone mémoire de la carte de la figure 1 selon l'invention.

La figure 3 est un schéma montrant une répartition d'éléments compteurs et indicateurs dans la zone mémoire de la figure 2.

La figure 4 est un schéma montrant une autre répartition d'éléments compteurs et indicateurs dans la zone mémoire de la figure 2.

La figure 5 est un schéma d'une autre mise en oeuvre de l'invention, ladite zone mémoire de la figure 2 contenant deux éléments indicateurs identiques.

La figure 1 montre un dispositif 10 à circuit intégré, une carte à circuit intégré dans l'exemple de réalisation représenté.

Cette carte 10 contient un élément 11 de commande (par exemple une unité centrale de traitement ou CPU), une zone mémoire 12 contenant une mémoire 14 de données, et un bloc 13 de contacts destiné à une connexion électrique avec par exemple un connecteur d'un lecteur de cartes .

Ladite zone mémoire 12 est représentée sur la figure 2. Elle contient un élément compteur CPT, une valeur seuil VS, un élément indicateur I et un moyen Mb de blocage, ledit élément indicateur étant apte à passer d'un premier état e1 à un second état e2 lorsque ledit élément compteur a atteint ladite valeur seuil. Au cours de l'utilisation de ladite carte, plusieurs événements peuvent se produire, un événement étant une action qui se produit dans ledit dispositif et qui aboutit à un résultat et dont on peut déterminer un nombre moyen d'occurrences dans l'utilisation dudit dispositif. Ainsi, par exemple, une

mise sous tension est un événement qui aboutit à l'envoi par la carte d'un message, couramment appelé réponse au reset. L'envoi d'un message signé est également un événement.

Au cours de l'utilisation d'une carte, pour une application particulière, on peut déterminer un nombre moyen d'événements qui peuvent se produire, par exemple du type envoi de messages signés. Ainsi, pour une application bancaire, sur une période d'environ deux ans représentant la durée de vie d'une carte bancaire, il y aura en moyenne trois cent messages signés pour une carte appartenant à un utilisateur utilisant sa carte environ trois fois par semaine et six cent pour un utilisateur l'utilisant environ cinq fois par semaine.

Sur la figure 2, l'élément compteur CPT compte au moins un nombre d'occurrences d'événements survenus dans la carte, le nombre d'occurrences de messages signés par exemple. Ledit élément compteur est susceptible d'atteindre la valeur seuil VS indicatrice d'un nombre maximum élevé d'occurrences desdits événements. Dans le cas où la carte à circuit intégré comporte une mémoire non réinscriptible (ROM), une mémoire inscriptible (EPROM) et une réinscriptible (EEPROM), la valeur seuil VS, étant fixe, pourra se trouver dans l'une de ces trois mémoires, lesdites mémoires étant au sens du brevet une mémoire de données, tandis que les éléments compteurs et indicateurs se trouveront dans une mémoire réinscriptible, leur valeur étant variable.

Dans le cadre de l'invention, ladite valeur seuil représente un nombre improbable d'occurrences desdits événements se produisant dans ledit dispositif lors d'un usage normal dudit dispositif. De manière à déceler un usage frauduleux du dispositif, ledit nombre maximum d'occurrences d'événements est choisi élevé car il représente un nombre improbable d'occurrences d'événements et ainsi, ledit nombre maximum élevé d'occurrences d'événements a une valeur supérieure à environ cent, préférentiellement supérieure à environ mille. Avec ces valeurs, on peut tenir compte de différents événements dans différentes

applications. Dans l'exemple précité, on sait qu'il est improbable que deux mille occurrences de messages signés puissent se produire entre la carte et un terminal bancaire. Aussi, dans ce cas, la valeur seuil aura comme définition le nombre deux mille. Si un tel cas se produit, il est fort probable qu'un fraudeur essaye de percer les secrets de ladite carte.

Aussi, pour prévenir les fraudes, lorsque ledit élément CPT a atteint ladite valeur VS, ledit élément indicateur I passe d'un premier état e1 à un second état e2, on dit que l'élément I passe d'un état passif à un état actif et, de plus, le dispositif selon l'invention prévoit que ladite zone mémoire 12 comporte un moyen Mb de blocage du fonctionnement dudit dispositif lorsqu'un élément indicateur est passé dans le second état e2. Ainsi, si on atteint deux mille occurrences de messages signés, un élément I est activé et ledit moyen Mb de blocage, après avoir vérifié l'état dudit élément I, bloque ladite carte qui ne peut plus soit, recevoir ou produire aucun événement de même nature que celui qui a activé l'élément indicateur, ici un événement de type message signé, soit, recevoir aucun événement ni effectuer aucune action quelle qu'elle soit. Dans le dernier cas, ladite carte est inutilisable et on dit couramment que la carte est muette.

Suivant un premier mode de réalisation dudit dispositif selon l'invention, un élément compteur est défini pour un unique événement.

Ainsi, sur la figure 3, l'élément compteur CPT1 est défini pour l'événement E1, l'élément CPT2 pour l'événement E2 et l'élément CPT3 pour l'événement E3.

Cependant, bien que des événements puissent être de nature différente, leurs nombres d'occurrences dans la vie d'une carte peuvent être du même ordre et par suite leurs nombres improbables d'occurrences peuvent être identiques. En conséquence, on peut vouloir les regrouper dans une même famille. Par exemple, on peut dire que l'envoi de messages signés fait partie de la même famille que l'envoi de messages cryptés. Aussi, suivant un deuxième mode de réalisation

dudit dispositif selon l'invention, un élément compteur est défini pour au moins deux événements, lesdits événements faisant partie d'une même famille. Ainsi, selon le schéma de la figure 4, les éléments compteurs CPT1 et CPT2 sont définis respectivement pour les deux familles d'événements (E1, E2, E3) et (E4, E5).

Dans les deux modes de réalisation, l'invention prévoit qu'une valeur seuil est définie pour chaque élément compteur. Ainsi, cela revient à avoir, soit les valeurs VS1, VS2 et VS3 respectivement associées à chaque événement comme dans le cas de la figure 3, soit les valeurs VS1 et VS2 respectivement associées à chaque famille d'événements comme dans le cas de la figure 4. Lorsqu'un élément CPT a atteint sa valeur seuil VS, des éléments indicateurs indiquent que le nombre maximum d'occurrences d'événements autorisés représenté par la valeur seuil VS a été atteint.

Dans les deux modes de réalisation précités, il existe deux variantes de réalisation desdits éléments indicateurs.

Dans une première variante de réalisation montrée à la figure 3, le dispositif selon l'invention prévoit qu'au moins un élément indicateur I est défini pour un unique élément compteur CPT. Ainsi, lorsque l'élément compteur CPT1 atteint la valeur seuil VS1, l'élément indicateur I1 passe dans le second état e12. Le moyen Mb de blocage vérifie l'état dudit élément I1 et dès que celui-ci est passé dans le second état, il bloque ladite carte, il en est de même avec les éléments I2 et I3.

Dans une deuxième variante de réalisation montrée à la figure 4, le dispositif selon l'invention prévoit qu'au moins un élément indicateur I est défini pour au moins deux éléments compteurs CPT. Ainsi, lorsqu'un des éléments CPT1 ou CPT2 atteint respectivement sa valeur seuil VS1 ou VS2, l'élément I1 passe de l'état e11 à l'état e12 ce qui indique qu'une fraude a eu lieu et en conséquence, le moyen Mb bloque la carte.

Ainsi, suivant ces deux modes de réalisation et ces deux variantes de réalisation associées, on limite le nombre d'occurrences d'événements se produisant dans une carte et par suite le nombre d'actions possibles sur la carte de la part d'un fraudeur.

Cependant, un fraudeur pourrait modifier l'état d'un élément indicateur en le rendant passif s'il était actif auparavant, avant même que le moyen Mb n'ait pu bloquer ladite carte et par suite il pourrait en toute impunité continuer à percer les secrets de ladite carte.

Aussi, ladite mémoire 14 de données dudit dispositif selon l'invention contient au moins deux éléments indicateurs identiques se trouvant à des emplacements non contigus de ladite mémoire de données, lesdits éléments étant rattachés au même ensemble d'éléments compteurs contenant un ou plusieurs compteurs suivant les deux variantes précitées en relation avec les figures 3 et 4. Comme le montre la figure 5, l'élément indicateur I'1 est identique à I1 dans la mesure où ils sont tous deux rattachés aux éléments CPT1 et CPT2 et ils passent en même temps d'un premier état à un second état lorsque n'importe lequel de ces deux éléments compteurs a atteint sa valeur maximum. De plus, lesdits éléments indicateurs se trouvent dans la mémoire 14 de données de ladite carte à des endroits non contigus ce qui permet d'éviter une fraude qui consisterait à changer l'état de tous les éléments indicateurs identiques actifs, ladite fraude étant facilitée par le fait que les éléments seraient à des emplacements très proches l'un de l'autre. Aussi, même si un fraudeur arrive à changer l'état d'un élément I en le rendant passif, les autres éléments indicateurs identiques resteront actifs car, dans ce cas, il sera improbable pour ledit fraudeur de trouver l'emplacement de tous les éléments indicateurs identiques.

Par ailleurs, le dispositif selon l'invention prévoit que ledit moyen Mb de blocage bloque le fonctionnement dudit dispositif lorsque l'état

d'un élément indicateur est différent de l'état d'un autre élément indicateur identique. L'action du fraudeur est ainsi contrée.

On notera que dans tous les cas, les valeurs des premiers états des éléments indicateurs pourront être équivalentes ou différentes entre elles. Il en sera de même pour les valeurs des seconds états.

C'est ainsi que grâce aux deux modes de réalisation, aux deux variantes de réalisation des éléments indicateurs et ainsi qu'au système d'éléments indicateurs identiques, le dispositif selon l'invention permet de mieux sécuriser la carte en limitant le nombre d'actions possibles sur celle-ci de la part d'un fraudeur.

REVENDICATIONS

1 - Dispositif à circuit intégré contenant une zone mémoire comprenant une mémoire de données, caractérisé en ce que ladite mémoire de données contient au moins un élément compteur, au moins un élément indicateur et au moins une valeur seuil, ledit élément compteur comptant, d'une part, au moins un nombre d'occurrences d'événements survenus dans ledit dispositif, et, étant, d'autre part, susceptible d'atteindre ladite valeur seuil indicatrice d'un nombre maximum élevé d'occurrences desdits événements, ledit élément indicateur étant apte à passer d'un premier état à un second état lorsque ledit élément compteur a atteint ladite valeur seuil.

2 - Dispositif selon la revendication 1, caractérisé en ce qu'un événement est une action qui se produit dans ledit dispositif et qui aboutit à un résultat et dont on peut déterminer un nombre moyen d'occurrences dans la vie dudit dispositif.

3 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que ladite valeur seuil représente un nombre improbable d'occurrences desdits événements se produisant dans ledit dispositif lors d'un usage normal dudit dispositif.

4 - Dispositif selon l'une des revendications précédentes, caractérisé en ce qu'une valeur seuil est définie pour chaque élément compteur.

5 - Dispositif selon l'une des revendications précédentes, caractérisé en ce qu'un élément compteur est défini pour un unique événement.

6 - Dispositif selon l'une des revendications 1 à 4, caractérisé en ce qu'un élément compteur est défini pour au moins deux événements.

7 - Dispositif selon l'une des revendications précédentes, caractérisé en ce qu'au moins un élément indicateur est défini pour un unique élément compteur.

8 - Dispositif selon l'une des revendications 1 à 6, caractérisé en ce qu'au moins un élément indicateur est défini pour au moins deux éléments compteurs.

9 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que ladite mémoire de données contient au moins deux éléments indicateurs identiques se trouvant à des emplacements non contigus de ladite mémoire de données.

10 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que ladite zone mémoire comporte un moyen de blocage du fonctionnement dudit dispositif lorsqu'un élément indicateur est passé dans le second état.

11 - Dispositif selon les revendications 9 et 10, caractérisé en ce que ledit moyen de blocage bloque le fonctionnement dudit dispositif lorsque l'état d'un élément indicateur est différent de l'état d'un autre élément indicateur identique.

12 - Dispositif selon l'une des revendications précédentes, caractérisé en ce que ledit nombre maximum élevé d'occurrences d'événements a une valeur supérieure à environ cent, préférentiellement supérieure à environ mille.

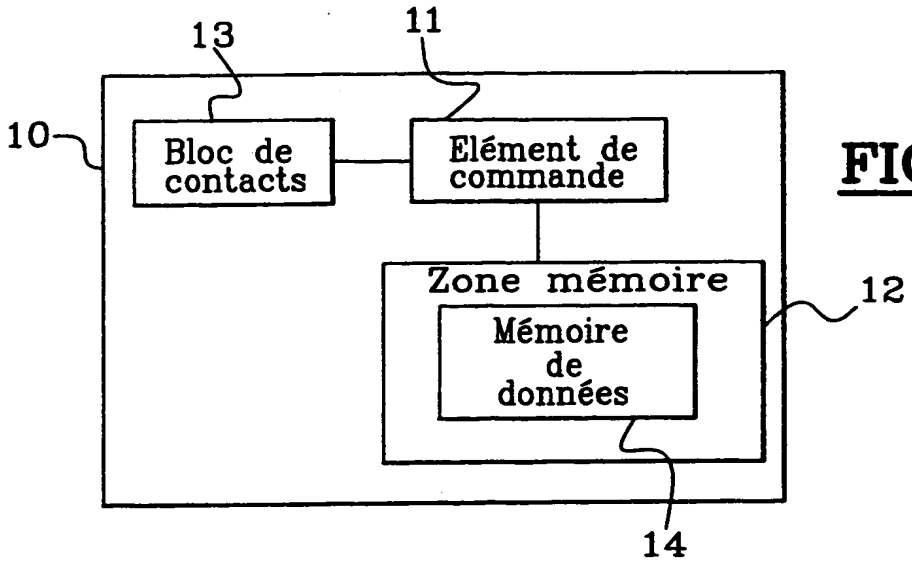

13
11
10
Bloc de contacts
Elément de commande
Zone mémoire
Mémoire de données
12
14

FIG.1

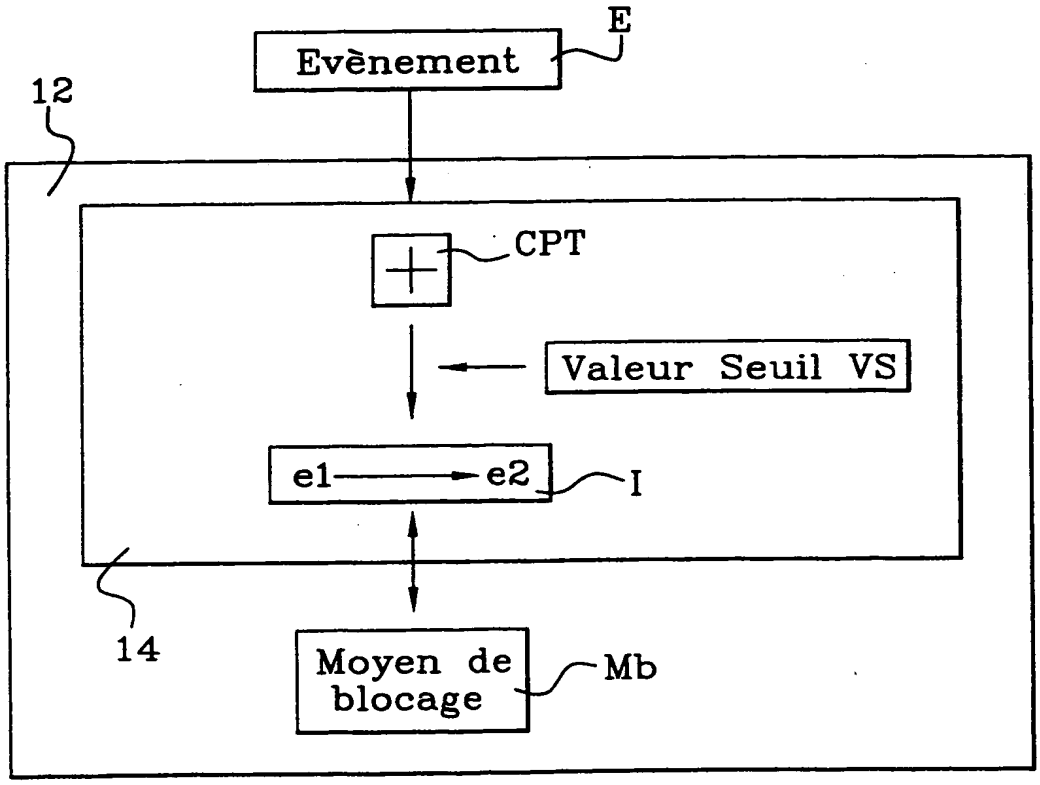
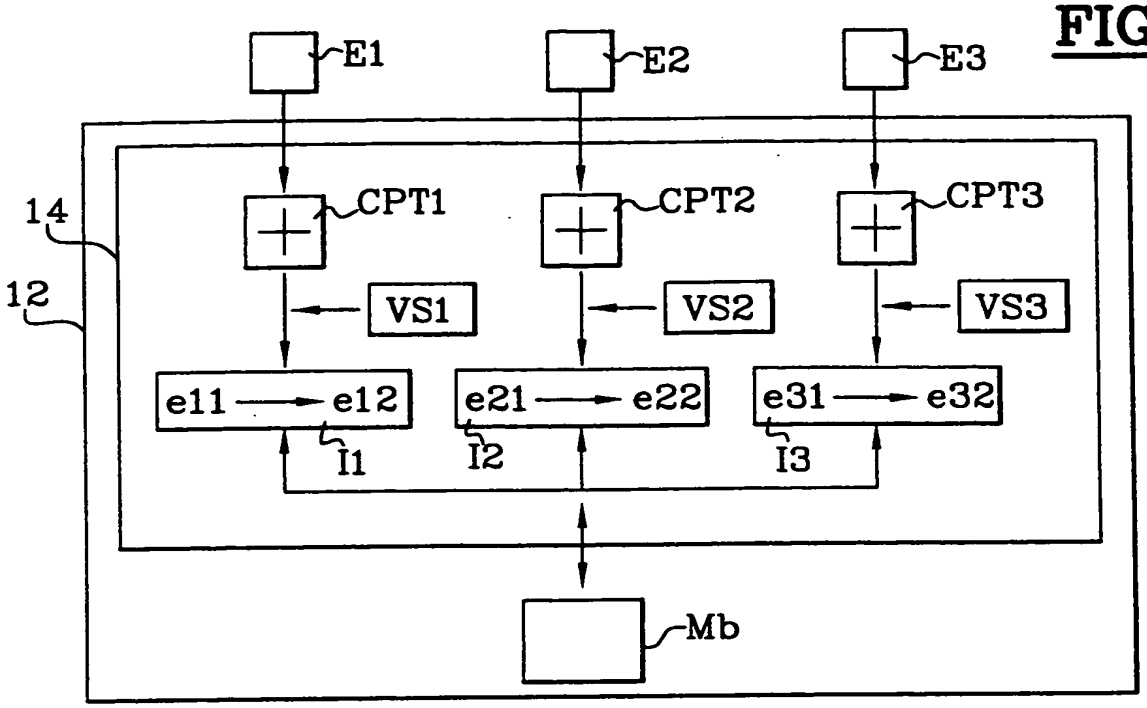

E
Evènement
12
CPT
Valeur Seuil VS
e1
e2
I
14
Moyen de blocage
Mb

FIG.2

FIG.3


E1
E2
E3
14
12
CPT1
CPT2
CPT3
VS1
VS2
VS3
e11
e12
e21
e22
e31
e32
I1
I2
I3
Mb

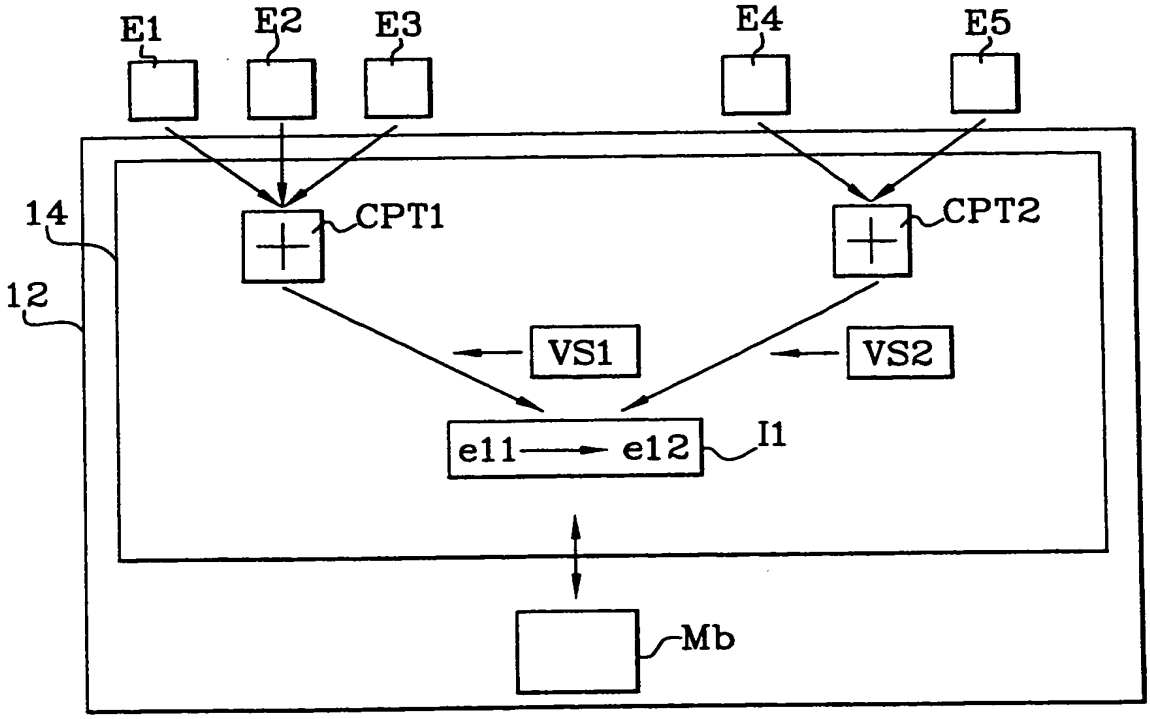

E1
E2
E3
E4
E5
14
12
CPT1
CPT2
VS1
VS2
e11
e12
I1
Mb

FIG.4

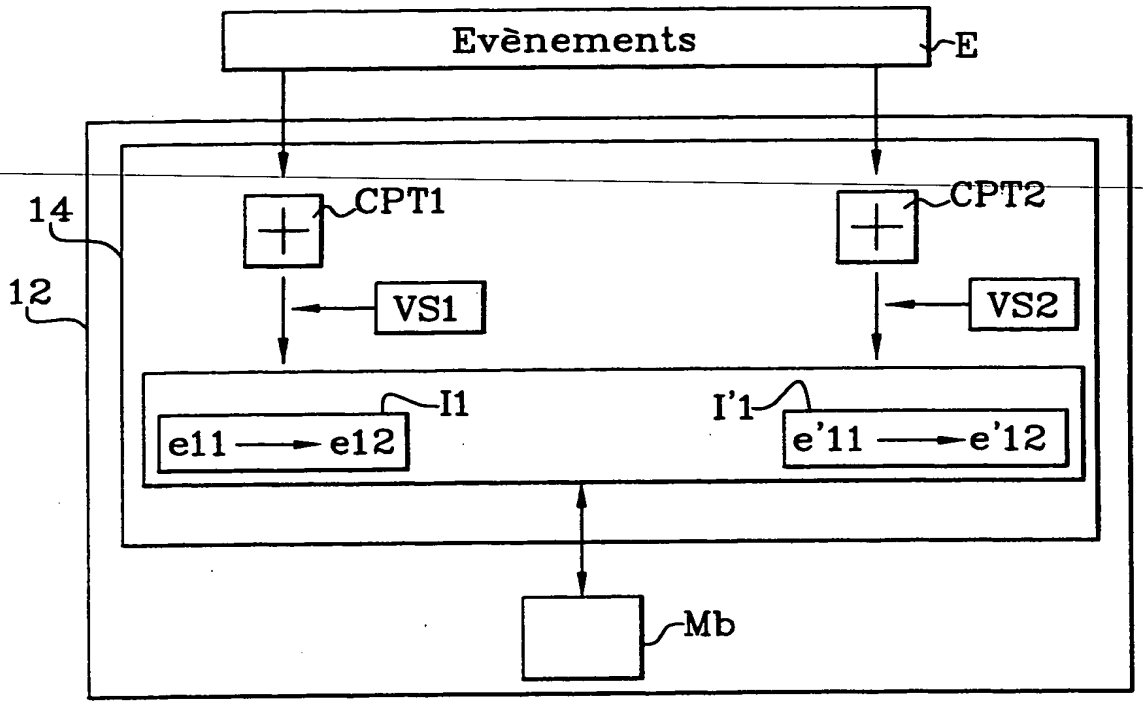


FIG.5